REMARKS/ARGUMENTS

Applicants have amended their claims to more particularly point out the claimed subject matter, and request the Examiner to reconsider and allow this case in view of the claim amendments and the following remarks.

Applicant's Interview Summary Record

Applicants appreciate the time devoted by USPTO personnel to the 1/19/06 personal interview. At the interview, inventor Emil Sturniolo explained that the widespread use of Virtual Private Networks (VPNs) on today's networks presents challenges to effective policy management. Because VPNs encrypt the traffic, it is not usually straightforward to perform policy management because it is not possible to monitor the content of traffic as it passes through the network .

Mr. Sturniolo explained that the exemplary illustrative non-limiting implementation herein provides a distributed model that can be used to enforce policy management at one, the other, or both ends of the communications path even though the communications are encrypted by a VPN tunnel. Mr. Sturniolo explained that the exemplary illustrative non-limiting implementation doesn't need to monitor packet traffic because the distributed policy management architecture, in one exemplary illustrative non-limiting implementation, understands which applications are running and which applications generated the communications It is therefore possible, explained Mr. Sturniolo, for the exemplary illustrative non-limiting implementation to dynamically

enforce policy management based on changing conditions even when a VPN or other mechanism is encrypting the traffic.

Mr. Sturniolo explained that such functionality can be useful in a variety of contexts including for example public safety. In one illustrative non-limiting example, when a police officer is dispatched, the police vehicle may need to move from one network to another (e.g., from a WIFI connection to a WAN connection). Under such circumstances, it would be possible for an exemplary illustrative non-limiting distributed policy management system as disclosed herein to permit only certain applications and not others to communicate over the WAN connection while permitting additional applications to communicate over the WIFI connection.

Mr. Sturniolo demonstrated certain mobility features of an exemplary illustrative commercial non-limiting implementation of assignee NetMotion's Mobility software technology. For the illustrative non-limiting demonstration, Mr. Sturniolo set up:

- a multi-homed application server that also hosted a DHCP server for two distinct IP-based communication paths A and B, as well as the NetMotion Wireless' Mobility server technology;
- two 802.11 wireless access points (1 and 2, one for each of the two respective communication paths A and B) and coupled to the multi-homed server using standard 802.3 interfaces; and

- one 802.3/802.11-capable mobile computing device that used a standard (Microsoft Windows) operating system with NetMotion Mobility agent installed.

For the first phase of the demonstration, Mr. Sturniolo established an application session from the mobile computing device to the application service (simple TCP services chargen capabilities - as outlined in RFC 864) over communication path **A** through access point **1** with the NetMotion Mobility agent disabled. Once the session was established and data was flowing to the mobile device, Mr. Sturniolo removed power from access point **1** to simulate a network disconnect or out-of-range condition. The mobile device's 802.11 adapter automatically associated itself with the access point **2** (as per the IEEE 802.11 specification) which was coupled to communication path **B**. Mr. Sturniolo showed the Examiners how the disconnect/reconnect sequence caused the mobile device to reacquire a network layer address associated with communication path **B** which is different than the address used to initiate the session. The Examiners observed how the change in network address caused the state of the application session to become ambiguous -- forcing the application to terminate the communications. This process demonstrated the behavior of typical prior art systems.

For a second phase of the illustrative non-limiting demonstration, Mr. Sturniolo restarted the test, but this time he activated the Netmotion Mobility agent on the mobile device. This instantiated a session with the Mobility server technology. Again, after the

application session was established via access point **1** to the application service through the Mobility server proxy, Mr. Sturniolo again removed the power simulating the network disconnect/out-of-range scenario. However this time, when the 802.11 device became associated with access point **2** and reacquired a different network layer address, the application session was not terminated. Assignee's exemplary illustrative non-limiting commercial implementation thus enabled the mobile device to migrate to different subnets without adversely affecting the application session.

Mr. Sturniolo explained that enabling this migration presents a new set of challenges for command and control. Mr. Sturniolo explained that, for example, a system administrator of such a system might want to further control access to a resource based on a number of parameters or events. One such parameter might be where the mobile device is physically coupled to the network.

To illustrate this, again Mr. Sturniolo restarted the test with the NetMotion's Mobility technology enabled. This time, however, Mr. Sturniolo also enabled an exemplary illustrative non-limiting distributed policy module of the system. He explained that the administrator might, as one illustrative non-limiting example, want to allow the application to communicate with the application server if/when connected over access point **1**, but not if/when connected over access point **2**. Again, after the application session was established, Mr. Sturniolo removed the power to access point **1**. At this point, the mobile device's 802.11 adapter became associated with access point **2**. However, the

Examiners observed that the application traffic for the session was stopped or blocked without terminating the session as in the first test. To demonstrate this, Mr. Sturniolo then reconnected the power to access point **1** and disconnected the power to access point **2** to force the mobile device to reassociated with access point **1**. Once the system had reestablished communications capability over access point **1**, the application session resumed and continued.

Mr. Sturniolo further explained that the administration and control of the policy can, in illustrative non-limiting exemplary implementations, be dynamic and distributed across one element or both the server and mobility agent and not limited to just physical connection location. Other parameters such as time, other mobility events, as well as application identity or invocation can be used to invoke command and control in illustrative non-limiting exemplary implementations.

Additional Response to Rejections

Further to the discussions during the personal interview, applicants have amended their claims to more particularly point out their claimed subject matter and to remove the objections/rejections under 35 USC §112. Two subsequent brief telephone conversations with Examiner Desir confirm that the claims herein amended as proposed fully patentably distinguish over the applied references. Exemplary support for new claim limitations may be found in the originally filed specification at for example page 79 and following and associated Figures.

Responding specifically to the non-enablement rejection set forth on pages 2-3, the phrase "based at least in part on the mobile computing device's ability to communicate" is fully supported by for example page 80, paragraph 234 ("MES communications capability ..."). With regard to the Examiner's concerns relating to "while the mobile computing device is unable to send IP datagrams over any network or subnetwork", see for example the disclosure of the Mobility Management Server beginning at paragraph 66.

During the personal interview, Mr. Sturniolo explained Ahmed does not teach or suggest a distributed policy management arrangement or method as recited in the amended claims. Mr. Sturniolo explained that Ahmed discloses a new mobility management addressing scheme that does not provide policy management as now claimed. Mr. Sturniolo further explained that the applied McCloghrie reference relies on packet inspection which could potentially be impractical or impossible in a VPN type deployment where traffic is encrypted. Mr. Sturniolo and the Examiners discussed the COPS approach of RFC2748 referenced by McCloghrie (see col. 15, line 22 et seq). Mr. Sturniolo pointed out that RFC2748 does not provide any enabling disclosure of mobility architectures as claimed herein. The applied secondary/tertiary references the Examiner has relied upon for specific purposes (St. Pierre, Goertzel, Pirot, Bowman-Amuah, Roach, Wiegel, Stewart et al, Ball, Kovacs, Inoue) do not supply the teachings missing from Ahmed and McCloghrie.

All outstanding issues have been addressed and this application is in condition for allowance. Should any minor issues remain outstanding, the Examiner should contact the undersigned at the telephone number listed below so they can be resolved expeditiously without need of a further written action.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /s/ Robert W. Faris

Robert W. Faris
Reg. No. 31,352

RWF:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile:. (703) 816-4100